REMARKS

Claims 1-20 are pending in the present application. Claims 21 and 22 were canceled. Claims 1-20 were amended. Reconsideration of the claims is respectfully requested.

Amendments were made to the specification to correct spelling errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

I. Telephone Interview with Examiner Nguyen on May 31, 2005

Applicants thank Examiner Nguyen for the courtesy extended to applicant's representative during the May 31, 2005 telephone interview. During the telephone interview, the examiner and applicants' representative discussed the cited prior art references contained in the Office Action and discussed amending the independent claims.

II. Objection to Claims

The examiner objects to claims 1, 4, and 5 because claims 1, 4, and 5 contain informalities. With regard to claim 1, 4, and 5, the examiner stated:

> As to claim 1 on page 14, line 7, "the the incoming request" should be "the incoming request."
> As to claim 4 on page 14, line 22, "the when the request" should be "the request."
> As to claim 5 on page 15, line 6, "a intrusion" should be "an intrusion" and line 9, "the the incoming request" should be "the incoming request."
> Appropriate correction is required.

Office Action, page 2.

In response, the claims have been rewritten according to the examiner's recommendations. Therefore, having made the appropriate corrections, the objection to claims 1, 4, and 5 have been overcome.

III. **35 U.S.C. § 102, Anticipation, Claims 1-16**

The examiner has rejected claims 1-16 under 35 U.S.C. § 102 as being anticipated by *Coley et al.*, U.S. Patent No. 5,826,014 ("*Coley*"). This rejection is respectfully traversed.

In rejecting the claims, the examiner stated:

> As to claims 1, 9, and 13, Coley discloses firewall system (i.e., server system) for protecting network elements connected to a public network comprising one or more source servers that store information (Fig. 2, elements 216, 218); a first server (Fig. 2, element 210), communicatively coupled to the one or more source servers and to the network; that receives the incoming request from the network (col. 7, lines 16-18) and the first server testing the incoming request (col. 7, lines 35-39) for an indicia (col. 6, lines 34-39; col. 8, lines 6-9) contained within the request that the request is not proper for the source servers to respond to the request (col. 7, lines 56-57), and passing the incoming request to the one or more source servers when the incoming request is valid (col. 9, lines 13-18).

Office Action, dated May 9, 2005, page 3.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). In this case, each and every feature of the claims at 1, 5, 9, and 13 are not shown in the cited reference as arranged in the claims.

Amended independent claim 1, which is representative of amended independent claims 5, 9, 13, and 17, with regard to similarly recited subject matter, reads as follows:

> 1. A server system that processes an incoming request for information from a user over a network, the server system comprising:
> one or more source servers that store the information;

> a first server, communicatively coupled to the one or more source servers and to the network, that receives the incoming request from the network; and
>
> the first server testing the incoming request for indicia contained within the request that the request is not valid for the one or more source servers to respond to the request, wherein the indicia includes a particular IP address in a context of prior requests, and wherein the context of prior requests is based on a number of requests for information from the particular IP address in a particular amount of time, and passing the incoming request to the one or more source servers when the incoming request is valid.

Coley does not teach the specific testing step as recited in amended claim 1. As amended, claim 1 tests for indicia in an incoming request for information from a user over a network, wherein the indicia includes a particular IP address in a context of prior requests, and wherein the context of prior requests is based on a number of requests for information from the particular IP address in a particular amount of time.

Coley teaches a system for:

> [p]roviding a firewall for isolating network elements from a publicly accessible network to which such network elements are attached. The firewall operates on a stand alone computer connected between the public network and the network elements to be protected such that all access to the protected network elements must go through the firewall. The firewall application running on the stand alone computer is preferably the only application running on that machine. The application includes a variety of proxy agents that are specifically assigned to an incoming request in accordance with the service protocol (i.e., port number) indicated in the incoming access request. An assigned proxy agent verifies the authority of an incoming request to access a network element indicated in the request.

Coley, Abstract.

In addition, *Coley* teaches that the verification tests performed by the proxy agent may involve a variety of checks including: determinations of valid destination addresses, determination of valid user, or user/password information, validity of an access in view of the time period of the access, presence of executable commands within an access request, or any combination of the latter, or like determinations. *Coley*, column 6, lines 33-40. Further, verification tests also may include characteristics of an access request, such as

source address, source host machine, and source user information. *Coley*, column 7, line 66 – column 8, line 9.

In contrast, the presently claimed invention in claim 1 tests an incoming request, in a context of prior requests, based on a number of requests for information from a particular IP address in a particular amount of time. In other words, in claim 1 requests for information are counted during a predetermined period of time from a specific IP address in the context of prior requests. When the number of requests from the specific IP address exceeds the predetermined limit during the identified time period, the request is not passed to the one or more source servers because the request is not valid as recited in claim 1. *Coley* does not teach or suggest that a verification test for an incoming information request includes checking the number of requests for information from a particular IP address in a particular amount of time in a context of prior requests. Furthermore, the examiner states, "Coley does not disclose the first server detecting an intrusion of the incoming request in the context of prior requests." *Office Action*, page 5. Consequently, *Coley* does not identically teach each and every element recited in claim 1 of the present invention. Accordingly, the rejection of independent claims 1, 5, 9, and 13 as being anticipated by *Coley* has been overcome.

In view of the above arguments, amended independent claims 1, 5, 9, and 13 are in condition for allowance. As a result, claims 2-4, 6-8, 10-12, and 14-16 are dependent claims depending on independent claims 1, 5, 9, and 13, respectively. Consequently, claims 2-4, 6-8, 10-12, and 14-16 also are allowable, at least by virtue of their dependence on allowable claims. Furthermore, these dependent claims also contain additional features not taught by *Coley*.

For example, amended dependent claim 4 of the present invention, which is representative of amended dependent claims 8, 12, and 16, reads as follows:

> 4. The server system of claim 1, wherein an incoming request is determined to be not valid when the request is for access to a particular resource.

As shown above, *Coley* teaches verification tests that check valid destination address, valid user or user/password, access in view of access time, presence of executable commands

within an access request, source address, source host machine, and source user information. *Coley*, column 6, lines 33-40 and column 7, line 66 – column 8, line 9. *Coley* makes no reference to determining if an access request is verified based upon accessing a particular resource. However, in rejecting dependent claim 4, the examiner stated:

> As to claims 4, 8, 12, and 16, Coley discloses the incoming request is determined to be not proper when the request is for access to a particular resource (col. 10, lines 53-55).

Office Action, page 3.

The passage cited by the examiner above states that "[i]f any incoming access request has a source address of a network element behind the firewall, that packet will be intercepted and discarded." *Coley*, column 10, lines 53-55. In other words, a device outside the protected network sends an access request with a machine address that is within the firewall protected network in order to gain access to the protected network. *Coley* does not teach or suggest that the incoming access request is for access to a particular resource as is recited in claim 4. An access request with an "IP spoofing" address as taught in *Coley* is distinguishable from a request for access to a particular resource as recited in claim 4. Therefore, Coley does not teach or suggest the limitation recited in dependent claim 4 of the present invention.

Accordingly, the rejection of claims 1-16 as being anticipated by *Coley* has been overcome.

IV. 35 U.S.C. § 103, Obviousness, Claims 17, 20, and 22

The examiner has rejected claims 17, 20, and 22 under 35 U.S.C. § 103 as being unpatentable over *Coley* in view of *Rowland*, U.S. Patent No. 6,405,318 ("*Rowland*"). This rejection is respectfully traversed.

In rejecting the claims, the examiner stated:

> As to claim 17, Coley discloses firewall system (i.e., server system) for protecting network elements connected to a public network comprising one or more source servers that store information (Fig. 2, elements 216, 218); a first server (Fig. 2, element 210), communicatively coupled to the one or more source servers and to the network; that receives the incoming request from the network (col. 7, lines 16-18), the first server

detecting an intrusion of the incoming request (col. 7, lines 54-55; line 64 to col. 8, line 16) and based on indicia (col. 6, lines 34-39; col. 8, lines 6-9) of the incoming request being proper, such indicia being associated with the incoming request, and the first server passing the incoming request to the one or more source servers when the indicia associated with the incoming request indicates that the incoming request is proper (col. 9, lines 13-18).

However, Coley does not disclose the first server detecting an intrusion of the incoming request in the context of prior requests.

Rowland discloses a computer implemented intrusion detection system and method that monitors a computer system in real-time for activity indicative of attempted or actual access by unauthorized persons or computers comprising the first server detecting an intrusion of the incoming request in the context of prior requests (Abstract).

It would have been obvious to one of ordinary skill in the art at the time of the invention to employ the use of detecting an intrusion of the incoming request in the context of prior requests in the system of Coley as Rowland teaches so as to effectively detect intrusions as they occur.

Office Action, page 5.

The examiner bears the burden of establishing a *prima facie* case of obviousness based on the prior art when rejecting claims under 35 U.S.C. § 103. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). For an invention to be prima facie obvious, the prior art must teach or suggest all claim limitations. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). The examiner has not met this burden because all of the features of these claims are not found in the cited references as believed by the examiner. Therefore, the combination of *Coley* and *Rowland* would not reach the presently claimed invention in these claims.

Amended independent claim 17 reads as follows:

17. A server system that processes an incoming request for information from a user over a network, the server system comprising:

one or more source servers that store the information;

a first server, communicatively coupled to the one or more source servers and to the network, that receives the incoming request from the network;

the first server detecting an intrusion by the incoming request based on indicia of the incoming request being improper, wherein the indicia includes a particular IP address in a context of prior requests, and wherein the context of prior requests is based on a number of requests for

information from the particular IP address in a particular amount of time; and

the first server passing the incoming request to the one or more source servers when the indicia associated with the incoming request indicates that the incoming request is proper.

Amended independent claims 1, 5, 9, and 13 include features similar to those in claim 17. The claim limitation language of canceled dependent claim 22 is incorporated into the above mentioned amended independent claims of the present invention. As shown above in the response to rejected claims 1, 5, 9, and 13, *Coley* does not teach or suggest all of the claim limitations as recited in amended independent claim 17. In particular, *Coley* does not teach or suggest that detecting an intrusion by an incoming request for information from a user over a network is based on indicia of the incoming request being improper, wherein the indicia includes a particular IP address in a context of prior requests, and wherein the context of prior requests is based on a number of requests for information from the particular IP address in a particular amount of time.

Rowland does not cure the deficiencies of *Coley*. *Rowland* teaches an intrusion detection system that automatically and dynamically builds user profile data (known as a signature) for each user (or alternatively, a class of users) that can be used to determine normal actions for each user to reduce the occurrence of false alarms and to improve detection. *Rowland*, Abstract. In rejecting canceled claim 22, which is incorporated into claim 17, the examiner stated, "[a]s to claim 22, Rowland discloses the context of prior requests is based on a number of requests for information from a particular IP address in a particular amount of time (col. 9, lines 21-24)." *Office Action*, page 6. The passage cited by the examiner to reject claim 22 teaches "[t]he odd login time module monitors user logins and attempts to spot 'unusual' login times based on past data collected for this user." *Rowland*, column 9, lines 21-23.

In other words, *Rowland* monitors user logins in the context of prior logins, whereas the present invention monitors a particular IP address in the context of prior requests as recited in claim 17. User login monitoring based upon previous logins is distinguishable from IP address monitoring based upon previous requests. In addition, *Rowland* monitors user login time of day, whereas the present invention monitors the number of requests over a specific quantity of time for a particular IP address. Monitoring

the time of day when a user usually logs in for the purpose of determining an unusual user login based upon normal user login patterns is not analogous to monitoring a predetermined length of time for the purpose of determining an intrusion based upon the number of requests for information from a particular IP address as recited in claim 17. Consequently, even though monitoring in *Rowland* is based upon prior user login patterns for determining odd or unusual login times in order to detect intrusion, *Rowland* monitoring is distinguishable from claim 17 testing because claim 17 testing is based upon the number of requests from a particular IP address in a particular amount of time to detect intrusion.

However, during the telephonic interview with Examiner Nguyen, Examiner Nguyen cited another *Rowland* passage in rejecting amended independent claim 17. The passage cited by the examiner during the telephonic interview teaches that, "[t]he multiple concurrent logins module will monitor logins and if it spots a user that is logged in more than once or is logged in from two or more separate domains/hosts, it will notify a control function and or the system administrator." *Rowland*, column 9, lines 13-17. In other words, *Rowland* teaches that a user is logged into a computer system when a hacker logs in utilizing the user's login, which means the user "is logged in more than once or is logged in from two or more separate domains/hosts" indicating intrusion. Thus, *Rowland* monitors multiple concurrent logins from multiple domains to detect suspicious activity. *Rowland*, column 9, lines 9-13.

In contrast, amended independent claim 17 of the present invention recites that detecting an intrusion by an incoming request is based on indicia of the incoming request being improper, wherein the indicia includes a particular IP address in a context of prior requests, and wherein the context of prior requests is based on a number of requests for information from the particular IP address in a particular amount of time. In other words, claim 17 recites multiple requests for information from a single IP address in the context of prior requests, whereas *Rowland* teaches two or more separate domains/hosts in the context of multiple concurrent user logins. Additionally, no need exists in the system of *Rowland* for monitoring prior concurrent user login history from two or more domains to determine intrusion because one event of multiple concurrent login signals suspicious activity, whereas intrusion detection in the present invention is based on a number of requests for information from a particular IP address in a particular amount of time in a

context of prior requests. As a result, *Rowland* does not teach or suggest all the claim limitations as recited in claim 17.

Therefore, since neither *Coley* nor *Rowland* teach or suggest that detecting an intrusion by an incoming request is based on a number of requests for information from a particular IP address in a particular amount of time as recited in claim 17, then the combination of *Coley* and *Rowland* cannot teach or suggest this recited feature. In view of the above arguments, amended independent claim 17, which contains the features of canceled dependent claim 22, is in condition for allowance. As a result, claims 18-20 are dependent claims depending on independent claim 17. Consequently, claims 18-20 also are allowable, at least by virtue of their dependence upon an allowable claim.

Accordingly, the rejection of claims 17 and 20 as being unpatentable over *Coley* in view of *Rowland* has been over come.

V. 35 U.S.C. § 103, Obviousness, Dependent Claims 18 and 21

The examiner has rejected claims 18 and 21 under 35 U.S.C. § 103 as being unpatentable over *Coley* in view of *Rowland* and further in view of *Bernhard et al.*, U.S. Patent No. 6,275,942 ("*Bernhard*").

With regard to the rejection of claim 18, this rejection is respectfully traversed. Claim 18 is a dependent claim dependent upon independent claim 17. As shown above, claim 17 is in condition for allowance. Consequently, claim 18 also is allowable, at least by virtue of its dependence upon an allowable claim.

As claim 21 has been canceled, the rejection of claim 21 is now moot. However, the feature of claim 21 has been incorporated into amended independent claims 1, 5, 9, 13, and 17. With regard to the rejection of canceled claim 21, the examiner stated, "[a]s to claim 21, Bernhard discloses the context of prior requests is based on a number of requests for information from a particular IP address (col. 8, lines 59-65)." *Office Action*, page 7.

As shown above, *Coley* and *Rowland* do not teach or suggest all of the limitations recited in claim 17, which is representative of claims 1, 5, 9, and 13. In particular, *Coley* and *Rowland* do not teach or suggest that detecting an intrusion by the incoming request is based on indicia of the incoming request being improper, wherein the indicia includes a particular IP address in a context of prior requests, and wherein the context of prior

requests is based on a number of requests for information from the particular IP address in a particular amount of time as recited in claim 17.

Bernhard does not cure the deficiencies of *Coley* and *Rowland*. *Bernhard* teaches a system for automatic response to computer system misuse using active response modules (ARMs). Upon receipt of an instance of the computer misuse from the intrusion detection system, each ARM linked to the misuse collects pertinent data from the intrusion detections system and invokes a response specified by the ARM class and the collected pertinent data. *Bernhard*, Abstract. Instances of misuse contemplated by the ARMs in *Bernhard* include an illegal login, jump, and privilege usage and access to files within a protected directory. *Bernhard*, column 4, lines 34-37.

The passage cited by the examiner to reject claim 21 above teaches that the misuses linked to an ARM involve, for example, a user who telnets into a computer system from a external site through the firewall and performs an operation which is considered a misuse. The firewall ARM, as part of its actions component, may then instruct the firewall to stop any further accesses from the originating IP address. *Bernhard*, column 8, lines 59-65. In other words, if a user in *Bernhard* performs "an illegal login, jump, or privilege usage and access to files within a protected directory," the user's IP address is denied further access to the computer system.

In contrast, claim 17 recites that detecting an intrusion by an incoming request is based on indicia of the incoming request being improper, wherein the indicia includes a particular IP address in a context of prior requests, and wherein the context of prior requests is based on a number of requests for information from the particular IP address in a particular amount of time. The types of misuse taught by *Berhard* are not in the context of prior requests as recited in claim 17. *Bernhard* does not teach or suggest tracking previous suspicious activity or prior occurrences of misuse to detect intrusion. In *Bernhard*, misuse is in the context of present events and not in the context of prior requests. In addition, even though *Bernhard* teaches denying access to a particular IP address for misuse, *Bernhard* does not teach or suggest that the misuse is based on a number of requests for information from the particular IP address in a particular amount of time in the context of prior requests as recited in claim 17. *Bernhard* makes no reference to detecting misuse based on a particular amount of time.

Hence, *Bernhard* does not teach or suggest all the claim limitations of independent claims 1, 5, 9, 13, and 17, which now incorporate the features of claim 21. In view of the above arguments, amended independent claims 1, 5, 9, 13, and 17 are in condition for allowance.

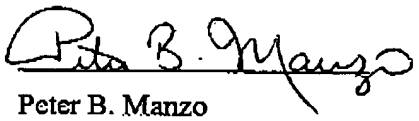
VI. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: June 8, 2005

Respectfully submitted,



Peter B. Manzo
Reg. No. 54,700
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants